# Khushboo Rani

1991 Kraft Dr. SW, Suite 2001, Blacksburg, Virginia 24061, Virginia Tech, USA.

kuchhu96@gmail.com • rkhushboo@vt.edu • Website • rani-khushboo • GoogleScholar • DBLP

## Profile

Postdoctoral Associate at Virginia Tech with 4+ years of postdoctoral research experience across three institutions (Virginia Tech, University of Florida, NUS Singapore). Co-PI on a funded ONR project ($986,606) on microcode-level security enforcement. Published in IEEE TCAD, IEEE TVLSI, DAC, and ICCD. Seeking research positions in secure processor architecture and AI systems security starting August 2026.

## Research Interest

My research focuses on secure processor design and architecture for AI systems — spanning microcode-level memory safety enforcement, side-channel attack mitigation (including Spectre-class transient execution vulnerabilities), and on-chip interconnect design for AI accelerators. I build deployable defenses on commodity hardware, enforcing memory compartmentalization with under 3% overhead on production workloads without requiring ISA extensions or application changes. My goal is to develop processor architectures that are fundamentally trustworthy as AI systems scale across heterogeneous compute fabrics.

## Honors and Awards

- Received Best Paper Award in ISED 2018
- Nominated for the Best Paper Award in VLSID 2019
- Received Grant from IARCS/ACM India for attending DAC 2020 conference in San Francisco, USA
- DAC Young Fellow 2020

## Education

**Indian Institute of Technology Guwahati, India** July 2012 – Jan 2021
*Ph.D. Computer Science & Engineering*

**Advisor:** Prof. Hemangee Kapoor

**Thesis Title:** LongLiveNoC: Wear Levelling, Write Reduction and Selective VC allocation for Long-lasting Dark Silicon aware NoC Interconnects

**Cochin University of Science and Technology, India** Aug 2005 – June 2009
*B. Tech. Computer Science & Engineering*

## Experience

**Department of ECE, Virginia Tech, USA** | *Postdoctoral Associate* May 2023 – Present
**Advisor:** Prof. Binoy Ravindran

Co-PI on a funded Office of Naval Research (ONR) project (TrustedCPU, $986,606) advancing microcode-level security enforcement on commodity x86-64 processors. Completed full control-flow enforcement implementation at the microcode layer; currently developing memory isolation mechanisms for spatial and temporal safety without ISA extensions or binary modifications. Contributed to DARPA/V-SPELLS and DARPA/BARC research on the IOCS framework for input-aware compartmentalization, enforcing fine-grained memory isolation with under 3% overhead on production workloads. Mentored 2 master's students on architecture and security research.

**Department of CISE, University of Florida, USA** | *Postdoctoral Associate* May 2022 – April 2023
**Advisor:** Prof. Prabhat Mishra

Served as lab lead for a team of 5-6 researchers on the DARPA/Synopsys Automated Implementation of Secure Silicon (AISS) program. Delivered a malicious hardware implant detection tool and cryptographic IP implementations for supply-chain trust during SoC design and fabrication. Results published at ICCD 2022 and presented at GOMACTech 2023. Mentored 1 PhD student and 2 undergraduate researchers within a one-year appointment.

**School of Computing, NUS, Singapore** | *Research Associate* May 2021 – Dec 2021
**Advisor:** Dr. Trevor Carlson

Contributed to hardware/software co-design research on mitigating Spectre-class transient execution attacks through compiler-assisted secure execution mechanisms and gem5-based microarchitectural modeling. Work conducted remotely during COVID-19 travel restrictions prior to joining University of Florida.

## Publications

### Journal

- Hansika Weerasena, Pan Zhixin, **Khushboo Rani** and Prabhat Mishra, "ML-based Flow Correlation Attack on Anonymous Routing and Lightweight Countermeasures for NoC-based SoCs," manuscript developed during postdoctoral research at the University of Florida (2022–2023).
- **Khushboo Rani** and Hemangee K. Kapoor, "Investigating Frequency Scaling, Non-Volatile, and Hybrid Memory Technologies for On-Chip Routers to Support the Era of Dark Silicon." In *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 40, no. 4 (2020): 633-645. DOI: 0.1109/TCAD.2020.3007555
- **Khushboo Rani** and Hemangee K. Kapoor, "Write Variation Aware Buffer Assignment for Improved Lifetime of Non-Volatile Buffers in On-Chip Interconnects." In *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 27, no. 9 (2019): 2191-2204. DOI: 10.1109/TVLSI.2019.2922471
- **Khushboo Rani** and Hemangee K. Kapoor, "Write-Variation Aware Alternatives to Replace SRAM Buffers with Non-Volatile Buffers in On-Chip Interconnects." In *IET Computers and Digital Techniques* 13, no. 6 (2019): 481-492. DOI: 10.1049/iet-cdt.2019.0039

### Conference

- **Khushboo Rani** and Binoy Ravindran, "Microcode-based Compartmentalization Enforcement for Fine-Grained Software Isolation," manuscript in preparation for submission.
  This work is supported by the Office of Naval Research (ONR) TrustedCPU project.
- Jae-Won Jang, Xiaoguang Wang, **Khushboo Rani**, David Narvaez, and Binoy Ravindran,"IOCS: Input-Oriented Object Compartmentalization for Memory Damage Containment," manuscript in preparation for submission.
  This work is supported by DARPA V-SPELLS and DARPA BARC programs.
- **Khushboo Rani**, Hansika Weerasena, Stephen A. Butler, Subodha Charles, and Prabhat Mishra, "Modeling and Exploration of Gain Competition Attacks in Optical Network-on-Chip Architectures." *Available: https://arxiv.org/abs/2303.01550*, 2023. DOI: 10.48550/arXiv.2303.01550
- Aruna Jayasena, **Khushboo Rani**, and Prabhat Mishra, "Efficient Finite State Machine Encoding for Defending Against Laser Fault Injection Attacks." *In 2022 IEEE 40th International Conference on Computer Design (ICCD)*, pp. 247-254. IEEE, 2022. DOI: 10.1109/ICCD56317.2022.00044
  This work was supported by the DARPA/Synopsys AISS program.
- **Khushboo Rani**, Sukarn Agarwal, and Hemangee K. Kapoor, "DidaSel: Dirty data based Selection of VC for effective utilization of NVM Buffers in On-Chip Interconnects." In *Proceedings of the ACM/IEEE International Symposium on Low Power Electronics and Design*, pp. 151-156. 2020. DOI: 10.1145/3370748.3406565

- **Khushboo Rani** and Hemangee K. Kapoor, "ZENCO: Zero-bytes based ENCOding for Non-Volatile Buffers in On-Chip Interconnects." In *2020 57th ACM/IEEE Design Automation Conference (DAC)*, pp. 1-6. IEEE, 2020. DOI: 10.1109/DAC18072.2020.9218620

- **Khushboo Rani** and Hemangee K. Kapoor, "Write Variation Aware Non-Volatile Buffers for On-Chip Interconnects." In *2019 32$^{nd}$ International Conference on VLSI Design and 18$^{th}$ International Conference on Embedded Systems (VLSID)*, pp. 7-12. IEEE, 2019. **(Best Paper Candidate).** DOI: 10.1109/VLSID.2019.00020

- **Khushboo Rani**, Sukarn Agarwal, and Hemangee K. Kapoor, "Non-blocking Gated Buffers for Energy Efficient on-chip Interconnects in the era of Dark Silicon." In *2018 8$^{th}$ International Symposium on Embedded Computing and System Design (ISED)*, pp. 74-79. IEEE, 2018. **(Best Paper Award).** DOI: 10.1109/ISED.2018.8704027

## Proposals

### Proposals Funded

- "TrustedCPU: Formally verified microcode customization for security exploit mitigation," Source: ONR, Dr. Binoy Ravindran (PI), Dr. Freek Verbeek (Co-PI), Dr. Khushboo Rani (Co-PI), Dr. Ruslan Nikolaev (Co-PI), Total amount: $986,606.00

### Proposals Submitted

- "Seal: Fully Automatic, Formally-verified Memory Isolation of Legacy Software with Application to Linux Device Drivers," Source: ONR, Dr. Binoy Ravindran (PI), Dr. Freek Verbeek (Co-PI), Dr. Jonas Haglund (Co-PI), Dr. Khushboo Rani (Co-PI), Total amount: $948,115.00

## Posters

- **Khushboo Rani**, Emma Andrews, Aruna Jayasena and Prabhat Mishra, "Defending Elliptic Curve Cryptography against Laser Fault Injection Attacks", In *GOMACTech*, 2023.

## PhD Forum

- VLSI Design 2020, Bangalore, India.
- DATE 2021, Virtual Conference & Exhibition.
- ASPDAC 2021, Virtual Conference.

## Teaching Assistant

### Indian Institute of Technology Guwahati, India

* Computer Architecture (CS223 : UG)
* Parallel Computer Architecture (CS527 : UG+PG)
* Computational Geometry (CS502 : UG+PG)
* Hardware Laboratory (CS224 : UG)
* System Software Lab (CS : UG)
* Theory of computation
* Introduction to Computing (CS101 : UG)

## Industry Experience

**Wipro Technologies, Bangalore India** | *Project Engineer* May 2010 – July 2012

Worked on two projects: (i) Nokia app development (ii) NetApp file system development and maintenance

## Skills

**Languages:** C/C++ (expert), Python (scripting — data extraction, automation), Shell scripting (benchmark automation)

**Operating Systems/Platforms:** Linux (primary), Unix, Docker (containerized simulation environments)

**Architecture Simulation:** GEM5, Garnet, Noxim, Booksim, DSENT (expert)

**Architecture Modeling Tools:** Orion, McPAT (used in publications), CACTI, NVSIM (NVM buffer configuration), HotSpot

**Security & Low-level Tools:** x86 Microcode (expert), HOL4 (x86 MMU modeling), Intel PIN (working knowledge)

**Hardware:** FPGA (basic)

**Other:** LaTeX (expert — papers, CV, statements)